Standard form of qudit stabilizer groups

Vlad Gheorghiu[1,*]

[1]*Department of Physics, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA*

(Dated: Version of January 10, 2011)

We investigate stabilizer codes with carrier qudits of equal dimension D, an arbitrary integer greater than 1. We prove that there is a direct relation between the dimension of a qudit stabilizer code and the size of its corresponding stabilizer, and this implies that the code and its stabilizer are dual to each other. We also show that any qudit stabilizer can be put in a standard, or canonical, form using a series of Clifford gates, and we provide an explicit efficient algorithm for doing this. Our work generalizes known results that were valid only for prime dimensional systems and may be useful in constructing efficient encoding/decoding quantum circuits for qudit stabilizer codes and better qudit quantum error correcting codes.

PACS numbers: 03.67.Mn, 03.67.Pp

I. INTRODUCTION

Quantum error correction is an important part of various schemes for quantum computation and quantum communication, and hence quantum error correcting codes, first introduced about a decade ago [1–3] have received a great deal of attention. For a detailed discussion see Ch. 10 of [4]. Most of the early work dealt with codes for qubits, with a Hilbert space of dimension $D = 2$, but qudit codes with $D > 2$ have also been studied [5–15]. They are of intrinsic interest and could turn out to be of some practical value.

The stabilizer formalism introduced by Gottesman in [16] for $D = 2$ (qubits) provides a compact and powerful way of generating quantum error correcting codes and extends the notion of linear classical error correcting codes [17] to the quantum domain. The stabilizer formalism has been generalized to cases where D is prime or a prime power, see e.g. [6, 12, 18, 19]. For composite D things are more complicated and there is no immediate and natural way of generalizing the notions. Our approach is to use generalized Pauli operators and stabilizers defined in the same way as in the prime case, see e.g. [13, 15]. This has the virtue that many (although not all) results that are valid in the prime dimensional case can be extended without too much difficulty to the more general composite case.

An important problem in the theory of stabilizer codes is what is their structure. Is there any "canonical" way of representing an arbitrary stabilizer code? If yes, can one use this fact for implementing various quantum error-correcting tasks? For prime D it turns out that there is such a standard form, see e.g. Ch. 10.5.7 of [4], and this allows for a better understanding of the error-correcting capabilities of the stabilizer code and also provides an efficient way of constructing encoding/decoding circuits for such stabilizer codes. For composite D we are not aware of any such standard form (except for the case of stabilizer codes over prime-power finite fields [12]), and the proof that such a form exists is one of the main results of the current article.

The reminder of the paper is organized as follows. Sec. II contains definitions of the generalized Pauli group and some quantum gates used later in the paper. It also defines rigorously qudit stabilizers and their corresponding stabilized subspaces (or codes), together with an alternative algebraic notation that we employ later. Sec. III contains our main results: a "size" theorem that relates the size of the stabilizer group to the dimension of its stabilized subspace, followed by a "structure" theorem that shows that any qudit stabilizer can be brought to a standard form through a series of elementary quantum gates. Finally, Sec. IV contains a summary, conclusions, and some open questions.

II. PRELIMINARY REMARKS AND DEFINITIONS

A. The generalized Pauli group on n qudits

We generalize Pauli operators to higher dimensional systems of arbitrary dimension D in the following way. The X and Z operators acting on a single qudit are defined as

$$Z = \sum_{j=0}^{D-1} \omega^j |j\rangle \langle j|, \quad X = \sum_{j=0}^{D-1} |j\rangle \langle j+1|, \qquad (1)$$

and satisfy

$$X^D = Z^D = I, \quad XZ = \omega ZX, \quad \omega = \mathrm{e}^{2\pi \mathrm{i}/D}, \qquad (2)$$

where *the addition of integers is modulo* D, as will be assumed from now on. For a collection of n qudits we use subscripts to identify the corresponding Pauli operators: thus Z_i and X_i operate on the space of qudit i. The Hilbert space of a single qudit is denoted by $\mathcal{H}$, and the Hilbert space of n qudits by $\mathcal{H}_n$, respectively. Operators of the form

$$\omega^\lambda X^{\mathbf{x}} Z^{\mathbf{z}} := \omega^\lambda X_1^{x_1} Z_1^{z_1} \otimes X_2^{x_2} Z_2^{z_2} \otimes \cdots \otimes X_n^{x_n} Z_n^{z_n} \qquad (3)$$

* vgheorgh@andrew.cmu.edu

will be referred to as *Pauli products*, where λ is an integer in $\mathbb{Z}_D$ and $\mathbf{x}$ and $\mathbf{z}$ are n-tuples in $\mathbb{Z}_D^n$, the additive group of n-tuple integers mod D. For a fixed n the collection of all possible Pauli products (3) form a group under operator multiplication, the *Pauli group* $\mathcal{P}_n$. If p is a Pauli product, then $p^D = I$ is the identity operator on $\mathcal{H}_n$, and hence the order of any element of $\mathcal{P}_n$ is either D or else an integer that divides D. While $\mathcal{P}_n$ is not Abelian, it has the property that two elements *commute up to a phase*:

$$p_1 p_2 = \omega^{\lambda_{12}} p_2 p_1, \tag{4}$$

with λ_{12} an integer in $\mathbb{Z}_D$ that depends on p_1 and p_2.

B. Generalization of qubit quantum gates to higher dimensions

In this subsection we define some one and two qudit gates generalizing various qubit gates. The qudit generalization of the Hadamard gate is the *Fourier gate*

$$\mathrm{F} := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} \omega^{jk} |j\rangle \langle k| \,. \tag{5}$$

For an invertible integer $q \in \mathbb{Z}_D$ (i.e. integer for which there exists $\bar{q} \in \mathbb{Z}_D$ such that $q\bar{q} \equiv 1 \bmod D$), we define a *multiplicative gate*

$$\mathrm{S}_q := \sum_{j=0}^{D-1} |j\rangle \langle jq| \,, \tag{6}$$

where qj means multiplication mod D. The requirement that q be invertible ensures that S_q is unitary; for a qubit S_q is just the identity.

For two distinct qudits a and b we define the CNOT gate as

$$\mathrm{CNOT}_{ab} := \sum_{j=0}^{D-1} |j\rangle \langle j|_a \otimes X_b^j = \sum_{j,k=0}^{D-1} |j\rangle \langle j|_a \otimes |k\rangle \langle k+j|_b \,, \tag{7}$$

the obvious generalization of the qubit Controlled-NOT, where a labels the control qudit and b labels the target qudit. Next the SWAP gate is defined as

$$\mathrm{SWAP}_{ab} := \sum_{j,k=0}^{D-1} |k\rangle \langle j|_a \otimes |j\rangle \langle k|_b \,. \tag{8}$$

It is easy to check that SWAP gate is hermitian and does indeed swap qudits a and b. Unlike the qubit case, the qudit SWAP gate is not a product of three CNOT gates, but can be expressed in terms of CNOT gates and Fourier gates as

$$\mathrm{SWAP}_{ab} = \mathrm{CNOT}_{ab} (\mathrm{CNOT}_{ba})^\dagger \mathrm{CNOT}_{ab} (\mathrm{F}_a^2 \otimes I_b), \tag{9}$$

Pauli operator	S_q	F
Z	Z^q	X
X	$X^{\bar{q}}$	Z^{D-1}

TABLE I. The conjugation of Pauli operators by one-qudit gates F and S_q ($\bar{q}$ is the multiplicative inverse of q mod D).

Pauli product	CNOT_{ab}	SWAP_{ab}	CP_{ab}
$I_a \otimes Z_b$	$Z_a \otimes Z_b$	$Z_a \otimes I_b$	$I_a \otimes Z_b$
$Z_a \otimes I_b$	$Z_a \otimes I_b$	$I_a \otimes Z_b$	$Z_a \otimes I_b$
$I_a \otimes X_b$	$I_a \otimes X_b$	$X_a \otimes I_b$	$Z_a^{D-1} \otimes X_b$
$X_a \otimes I_b$	$X_a \otimes X_b^{D-1}$	$I_a \otimes X_b$	$X_a \otimes Z_b^{D-1}$

TABLE II. The conjugation of Pauli products on qudits a and b by two-qudit gates CNOT, SWAP and CP. For the CNOT gate, the first qudit a is the control and the second qudit b the target.

with

$$(\mathrm{CNOT}_{ba})^\dagger = (\mathrm{CNOT}_{ba})^{D-1} = (I_a \otimes \mathrm{F}_b^2) \mathrm{CNOT}_{ba} (I_a \otimes \mathrm{F}_b^2). \tag{10}$$

Finally we define the generalized Controlled-phase or CP gate as

$$\mathrm{CP}_{ab} = \sum_{j=0}^{D-1} |j\rangle \langle j|_a \otimes Z_b^j = \sum_{j,k=0}^{D-1} \omega^{jk} |j\rangle \langle j|_a \otimes |k\rangle \langle k|_b \,. \tag{11}$$

The CP and CNOT gates are related by a local Fourier gate, similar to the qubit case

$$\mathrm{CNOT}_{ab} = (I_a \otimes \mathrm{F}_b) \mathrm{CP}_{ab} (I_a \otimes \mathrm{F}_b)^\dagger, \tag{12}$$

since F maps Z into X under conjugation (see Table I).

The gates F, S_q, SWAP, CNOT and CP are unitary operators that map Pauli operators to Pauli operators under conjugation, as can be seen from Tables I and II. They are elements of the so called *Clifford group* on n qudits [20, 21], the group of n-qudit unitary operators that leaves $\mathcal{P}_n$ invariant under conjugation, i.e. if O is a Clifford operator, then $\forall p \in \mathcal{P}_n$, $OpO^\dagger \in \mathcal{P}_n$. From Tables I and II one can easily deduce the result of conjugation by F, S_q, SWAP, CNOT and CP on *any* Pauli product.

C. Qudit stabilizer codes

Relative to this group we define a *stabilizer* code $\mathcal{C}$ to be a $K \geq 1$-dimensional subspace of the Hilbert space satisfying three conditions:

C1: There is a subgroup $\mathcal{S}$ of $\mathcal{P}_n$ such that for *every* s in $\mathcal{S}$ and *every* $|\psi\rangle$ in $\mathcal{C}$

$$s|\psi\rangle = |\psi\rangle \tag{13}$$

C2: The subgroup $\mathcal{S}$ is maximal in the sense that every s in $\mathcal{P}_n$ for which (13) is satisfied for all $|\psi\rangle \in \mathcal{C}$ belongs to $\mathcal{S}$.

C3: The coding space $\mathcal{C}$ is maximal in the sense that any ket $|\psi\rangle$ that satisfies (13) for every $s \in \mathcal{S}$ lies in $\mathcal{C}$.

If these conditions are fulfilled we call $\mathcal{S}$ the *stabilizer* of the code $\mathcal{C}$. That it is Abelian follows from the commutation relation (4), since for $K > 0$ there is some nonzero $|\psi\rangle$ satisfying (13).

Note that one can always find a subgroup $\mathcal{S}$ of $\mathcal{P}_n$ satisfying C1 and C2 for any subspace $\mathcal{C}$ of the Hilbert space, but it might consist of nothing but the identity. Thus it is condition C3 that distinguishes stabilizer codes from nonadditive codes. A stabilizer code is uniquely determined by $\mathcal{S}$ as well as by $\mathcal{C}$, since $\mathcal{S}$ determines $\mathcal{C}$ through C3, so in a sense the code and its stabilizer are dual to each other.

D. Stabilizer generators and equivalent algebraic descriptions of qudit stabilizer codes

Any stabilizer group can be compactly described using a set of *group generators*. A generator corresponds to a specific Pauli product and can be completely specified, see (3), by a phase λ and two n-tuples in $\mathbb{Z}_D^n$, $\mathbf{x}$ and $\mathbf{z}$. A collection of k generators can therefore be represented by a k-component *phase vector* over $\mathbb{Z}_D$ (that contains all k phases) and a $k \times 2n$ *parity-check matrix* over $\mathbb{Z}_D$ with rows corresponding to the stabilizer generators. For example, the stabilizer

$$\mathcal{S} = \langle \omega^2 X_1^3 Z_2^2, X_2^2 \rangle \tag{14}$$

corresponds to the phase vector $(2, 0)$ and parity-check matrix

$$\mathbf{S} = \left(\begin{array}{cc|cc} 3 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 \end{array}\right). \tag{15}$$

The angular brackets in (14) means "group generated by", i.e. the group obtained by all possible products of the group generators. We call the left $k \times n$ block of the parity-check matrix the X-block, and the right $k \times n$ the Z-block, since they describe the X and Z parts of the stabilizer generators, respectively.

Note that if D is a prime number, any stabilizer group can be described using no more than n generators. However, in composite dimensions one can have more that n generators but no more than $2n$. For example, in $D = 4$, the $n = 1$ qudit stabilizer $\mathcal{S} = \langle X^2, Z^2 \rangle$ is generated by 2 (and not 1) elements and specify the stabilizer state $(|0\rangle + |2\rangle)/\sqrt{2}$. There is no way of representing this state using only 1 generator; Z^2 by itself stabilizes both $|0\rangle$ and $|2\rangle$, hence everything in their span, so the condition C3 is not satisfied, i.e. the coding space is not maximal. The same kind of analysis holds for X^2. A more rigorous analysis can be done using the Theorem 1 of Sec. III, which implies for this example that the size of the stabilizer group must be equal to 4, hence it must be generated by a single generator of order 4 or two generators each of order 2. By inspection it is easy to rule out the first case, so indeed one *must* use 2 generators.

Gate	X-part	Z-part
SWAP_{ab}	Interchange columns a and b	Interchange columns $a+n$ and $b+n$
$\mathrm{S}_{q,a}$	Multiply column a by invertible integer q^{-1}	Multiply column $a+n$ by invertible integer q
$(\mathrm{CNOT}_{ab})^m$	Substract m times column a from column b	Add m times column $b+n$ to column $a+n$

TABLE III. Conjugation by the above quantum gates correspond to elementary column operations on the X and Z parts of the parity-check matrix of a stabilizer code. For the CNOT gate, the first qudit a is the control and the second qudit b the target. The integer exponent m means CNOT applied m times (or, equivalently, the m-th power of the CNOT gate).

A conjugation of a stabilizer group by a Clifford operation will change the stabilizer group to an isomorphic group. This will correspond to a *column operation* on the parity-check matrix of the stabilizer, together with a transformation of the phase vector. On the other hand, the generator description of a stabilizer group is not unique: one can multiply a generator by another one and still get the same group. This kind of operation corresponds to a *row operation* on the parity-check matrix, again keeping in mind that in general the phase vector will modify. From now on for the sake of simplicity we will ignore the phase vector, although in real applications one has to keep track of the phases.

The following represent what we call *elementary row/column* operations: a) interchanging of rows/columns, b) multiplication of a row/column by an *invertible* integer, c) addition of any multiple of a row/column to a *different* row/column. The column operations can be realized by conjugations of the stabilizer by the Clifford operations in Table III, and the row operations just ensure that the stabilizer group remains the same, i.e. the new set of generators generate the same stabilizer group and not a smaller one.

III. SIZE-STRUCTURE THEOREMS

The following theorem generalizes to composite D a well-known result for prime D that relates the size of the stabilizer group to the dimension of its stabilizer subspace. Although the composite D result of our next theorem may have been known by the community (see e.g. the claim near the end of Sec. 3.6 of [16]), we have not yet seen a proof of it.

Theorem 1 (Size)**.** *Let $\mathcal{C}$ be an n-qudit stabilizer code*

with stabilizer $\mathcal{S}$. Then

$$K \times |\mathcal{S}| = D^n, \tag{16}$$

where K is the dimension of $\mathcal{C}$, $|\mathcal{S}|$ is the size (or order) of the stabilizer group $\mathcal{S}$ and D is the dimension of the Hilbert space of one carrier qudit.

Proof. Define

$$P := \frac{1}{|\mathcal{S}|} \sum_{s \in \mathcal{S}} s. \tag{17}$$

We will first show that P is the projector onto $\mathcal{C}$.

It follows at once that

$$P = P^\dagger = P^2, \tag{18}$$

where the equalities follow from the group property of $\mathcal{S}$, so P is an orthogonal projector. Let $|\psi\rangle$ be an arbitrary vector that belongs to the stabilizer code $\mathcal{C}$. Then $s|\psi\rangle = |\psi\rangle \ \forall s$ (see the condition C1 (13) that a stabilizer code must satisfy), which together with (17) yields

$$P|\psi\rangle = |\psi\rangle. \tag{19}$$

Therefore the subspace $\mathcal{W}$ onto which P projects includes $\mathcal{C}$, $\mathcal{C} \subset \mathcal{W}$. Let us now choose an arbitrary $|\phi\rangle \in \mathcal{W}$. Then

$$|\phi\rangle = P|\phi\rangle = \frac{1}{|\mathcal{S}|} \sum_{s \in \mathcal{S}} s|\phi\rangle. \tag{20}$$

Multiply (20) on the left by some arbitrary $t \in \mathcal{S}$ and use the group property of $\mathcal{S}$ to get

$$\begin{aligned} t|\phi\rangle = tP|\phi\rangle &= \frac{1}{|\mathcal{S}|} \sum_{s \in \mathcal{S}} ts|\phi\rangle = \frac{1}{|\mathcal{S}|} \sum_{s \in \mathcal{S}} s|\phi\rangle \\ &= P|\phi\rangle = |\phi\rangle. \end{aligned} \tag{21}$$

Since t was arbitrary we arrived at the conclusion that

$$t|\phi\rangle = |\phi\rangle, \forall t \in \mathcal{S}, \tag{22}$$

which proves that $|\phi\rangle$ belongs to the stabilizer subspace $\mathcal{C}$, and this implies that $\mathcal{W} \subset \mathcal{C}$. Hence P projects strictly onto $\mathcal{C}$ (and not on some larger subspace that includes $\mathcal{C}$). Its trace is just the dimension K of $\mathcal{C}$,

$$\mathrm{Tr}(P) = K = \frac{1}{|\mathcal{S}|} D^n. \tag{23}$$

where we have used that fact that all Pauli products in (17) are traceless except the identity (that must belong to the sum, since $\mathcal{S}$ is a group), of trace D^n. This concludes the proof. □

When D is a composite integer the dimension of the stabilizer code does not have to be a power of D any more (as was the case in the prime D case), but can be any divisor of D^n. As an illustrative example, consider the 1-qudit stabilizer generated by $\mathcal{S} = \langle Z^2 \rangle$ in $D = 4$. It is obvious that $\mathcal{S}$ stabilizes a $K = 2$-dimensional code $\mathcal{C}$=span$\{|0\rangle, |2\rangle\}$, and the size of the stabilizer is $|\mathcal{S}| = 2$.

Whenever $D = 2$ (qubits) it was shown in [16] (see also Ch. 10.5.7 of [4] for a detailed discussion) that any stabilizer code can be put into a "standard form" or "canonical form", and this is very useful for constructing encoding/decoding quantum circuits for stabilizer codes. This result can be generalized at once to prime D. However, for composite dimensions, it is not so obvious how to do the generalization, and the main technical difficulty is that $\mathbb{Z}_D$ is a ring (and not a field) and therefore some integers are not invertible. However, in the following Theorem we show that one can still apply a technique similar to a Gaussian elimination over $\mathbb{Z}_D$ and put any composite D stabilizer code into a standard form similar to the one of prime D case.

Theorem 2 (Standard form)**.** *Let $\mathcal{C}$ be a K dimensional n-qudit stabilizer code with stabilizer $\mathcal{S}$ generated by $k \leqslant 2n$ generators and with corresponding parity-check matrix $\boldsymbol{S}$ of size $k \times 2n$. Then $\mathcal{S}$ is isomorphic through a conjugation by a Clifford operation to another stabilizer $\mathcal{S}'$, with parity check matrix $\boldsymbol{S}$' in* standard form

$$\boldsymbol{S}\text{'} = \begin{array}{c} \\ r\{ \\ k-r\{ \end{array} \left(\begin{array}{cc|cc} \overbrace{\boldsymbol{M}}^{r} & \overbrace{\boldsymbol{0}}^{n-r} & \overbrace{\boldsymbol{Z}_1}^{r} & \overbrace{\boldsymbol{Z}_3}^{n-r} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{Z}_2 & \boldsymbol{Z}_4 \end{array} \right), \tag{24}$$

where the dimensions of the block matrices are indicated by curly brackets.

Here $\boldsymbol{M} = diag(m_1, \ldots, m_r)$, with $1 \leqslant r \leqslant n$, is a diagonal matrix with all $m_j \neq 0$ divisors of D. The matrices $\boldsymbol{Z}_1$ and $\boldsymbol{Z}_2$ satisfy

$$\boldsymbol{Z}_1 \boldsymbol{M} = \boldsymbol{M} \boldsymbol{Z}_1^T \quad mod\ D, \tag{25}$$

$$\boldsymbol{Z}_2 \boldsymbol{M} = \boldsymbol{0} \quad mod\ D, \tag{26}$$

where T in the exponent denotes the transpose, and the matrix $\boldsymbol{Z}_4$ is a diagonal rectangular matrix, with diagonal elements divisors of D. The notation $\boldsymbol{0}$ denotes the zero-block matrix.

Proof. The key ingredient of the proof is the Smith normal form: through a sequence of elementary row/column operations mod D (see the discussion at the end of Sec. III, a matrix M over $\mathbb{Z}_D$ can be converted to the Smith normal form [22, 23] (see also Sec. IV.B of [15] for an example)

$$\mathbf{M'} = \mathbf{V} \cdot \mathbf{M} \cdot \mathbf{W}, \tag{27}$$

where $\mathbf{V}$ and $\mathbf{W}$ are invertible (in the mod D sense) square matrices, and $\mathbf{M'}$ is a diagonal rectangular matrix, with diagonal elements divisors of D. The matrix $\mathbf{V}$ represents the row operations and $\mathbf{W}$ the column operations.

Note that in our case all necessary column operations can be realized by the corresponding gates in Table III,

and, more important, they *do not mix* the X and Z parts of the parity-check matrix. Therefore, without being concerned with what happens to the Z part of the parity-check matrix $\mathbf{S}$, we can put its X part in the Smith normal form (again we stress that this can be done because the Z part to not interfere with the X part), and arrive at a parity-check matrix of the form (24). Next by another series of Clifford gates acting only on the last $(n-r)$ qudits one can further put the $\mathbf{Z}_4$ matrix in its Smith normal form, without modifying the X part of the parity-check matrix (which is already in Smith normal form), since there are only zeros on the last $n-r$ columns of the X part; note that the row operations are done on the last $k-r$ rows, and again do not modify the X part of the parity-check matrix. Since the elementary row operations do not change the stabilizer group and the elementary column operations correspond to Clifford gates, see Table III, our whole transformation from $\mathcal{S}$ to $\mathcal{S}'$ is a conjugation by a Clifford operation.

Finally note that conjugation by Clifford operations do not change the commutation relations. It is easy to deduce from (3) that two Pauli products described by $(\mathbf{x}|\mathbf{z})$ and $(\mathbf{x'}|\mathbf{z'})$ commute if and only if

$$\mathbf{x}\cdot\mathbf{z'} = \mathbf{z}\cdot\mathbf{x'} \mod D, \tag{28}$$

where the dot represents the usual inner product of two vectors in $\mathbb{Z}_D$, e.g. the sum of the products of individual components. Using (28) we observe at once that the final set of generators commute if and only if (25) and (26) hold, and this concludes the proof. □

It is proved in [23] that a $M \times N$ matrix can be reduced to the Smith form in only $\mathcal{O}(M^{\theta-1}N)$ operations from $\mathbb{Z}_D$, where θ is the exponent for matrix multiplication over the ring $\mathbb{Z}_D$, i.e. two $M \times M$ matrices over $\mathbb{Z}_D$ can be multiplied in $\mathcal{O}(M^\theta)$ operations from $\mathbb{Z}_D$. Using standard matrix multiplication $\theta = 3$, but better algorithms [24] allow for $\theta = 2.38$. This ensures that our procedure outlined above is computationally efficient.

Whenever D is prime its only non-zero divisor is 1, hence $\mathbf{M}$ is just the identity matrix and $\mathbf{Z}_4$ has only 0's and 1's on the diagonal. From (25) and (26), $\mathbf{Z}_1$ must be symmetric and $\mathbf{Z}_2$ must be the zero matrix, hence our standard form reduces to the one known for prime D's [16]. [1]

Also for prime D it was proven in [12] that any stabilizer group $\mathcal{S}$ is Clifford equivalent to another stabilizer $\mathcal{S}'$ generated only by Z's, $\mathcal{S}' = \langle Z_1, Z_2, \ldots, Z_k\rangle$ [2]. This result is not true for composite D's, and one easy to see counterexample is the 1-qudit stabilizer $\mathcal{S} = \langle X^2, Z^2\rangle$ in $D = 4$, mentioned before in Sec. II D.

IV. CONCLUSIONS AND OPEN QUESTIONS

We studied stabilizer codes with carrier qudits of composite dimension D. We proved a size theorem that relates the size of the stabilizer group to the dimension of its stabilized code. Furthermore, we have shown that any stabilizer code can be put in a standard (canonical) form through a series of Clifford gates, and we provided a constructive algorithm. Our result generalizes what was known in the prime D case and may be useful in constructing efficient encoding/decoding quantum circuits, following the procedures outlined in [16].

Our approach was based on the generalized Pauli group introduced by (1) and (2). However, for composite dimensions, this is not the only way of introducing Pauli operators. An alternative way is to split the dimension in its prime-power factors which will then induce a natural splitting of the carrier qudits in subsystems of prime-power dimensions. In each of these subsystems then one can define Pauli operators using finite fields (any finite field is isomorphic to a prime-power canonical representation), as done e.g. in [12]. Although this is the scope of future work, we think it may be useful since in a sense "decouples" the stabilizer into prime-power subsystems, and the latter can be put into standard forms as done in [12]. One can then use previously known results for stabilizers over finite fields to study various properties of composite D stabilizers, and this may help building more efficient quantum error correcting codes.

Finally one may ask if there exist alternative standard forms of qudit stabilizer codes, perhaps more useful that the one presented here. We do not know if such forms exist, and searching for them may be worthwhile.

ACKNOWLEDGMENTS

The research described here received support from the Office of Naval Research and from the National Science Foundation through Grant No. PHY-0757251.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[2] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[3] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 5th ed. (Cambridge University Press, Cambridge, 2000).

[5] E. M. Rains, IEEE Trans. Inf. Theory **45**, 1827 (1999).

[6] A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**, 3065 (2001).

[7] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**,

[1] Except the fact that we also perform column operations by Clifford conjugations, which further simplifies the standard form of [16].

[2] Their result is more general and holds for any finite field, provided one redefines the Pauli operators in (1) accordingly.

012308 (2001).
[8] Dirk Schlingemann, "Stabilizer codes can be realized as graph codes," E-print arXiv:quant-ph/0111080.
[9] D. Schlingemann, "Logical network implementation for cluster states and graph codes," E-print arXiv:quant-ph/0202007.
[10] M. Grassl, T. Beth, and M. Roetteler, Int. J. Quantum Inf. **2**, 55 (2004).
[11] V. Arvind, P. P. Kurur, and K. R. Parthasarathy, "Non-stabilizer quantum codes from abelian subgroups of the error group," E-print arXiv:quant-ph/0210097.
[12] M. Grassl, M. Roetteler, and T. Beth, "Efficient Quantum Circuits for Non-Qubit Quantum Error-Correcting Codes," E-print arXiv:quant-ph/0211014.
[13] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **78**, 042303 (2008).
[14] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh, Phys. Rev. A **78**, 012306 (2008).
[15] V. Gheorghiu, S. Y. Looi, and R. B. Griffiths, Phys. Rev. A **81**, 032326 (2010).
[16] D. Gottesman, "Stabilizer codes and quantum error correction," E-print arXiv:quant-ph/9705052.
[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Mathematical Library, Amsterdam, 1977).
[18] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, IEEE Trans. Inf. Theory **51**, 4892 (2006).
[19] X. Chen, B. Zeng, and I. L. Chuang, Phys. Rev. A **78**, 062315 (2008).
[20] D. Gottesman, "Fault-Tolerant Quantum Computation with Higher-Dimensional Systems," E-print arXiv:quant-ph/9802007.
[21] E. Hostens, J. Dehaene, and B. D. Moor, Phys. Rev. A **71**, 042315 (2005).
[22] M. Newman, *Integral Matrices* (Academic Press, New York, 1972).
[23] A. Storjohann, in *ISSAC '96: Proceedings of the 1996 international symposium on Symbolic and algebraic computation* (ACM, New York, NY, USA, 1996) pp. 267–274.
[24] D. Coppersmith and S. Winograd, in *STOC '87: Proceedings of the nineteenth annual ACM symposium on Theory of computing* (ACM, New York, NY, USA, 1987) pp. 1–6.